

GUIDELINES FOR SOCIAL MEDIA USE

I. PURPOSE

The State recognizes that the internet provides unique avenues to participate in discussions and share information with customers and the public. Social Media in particular offer ways to communicate with a broad range of individuals and groups who are using the internet rather than traditional forms of media for communicating and learning.

Social Media use will vary from agency to agency, depending upon an agency's mission. Each agency should carefully select the Social Media that will best serve its needs.

Like all communication tools, Social Media should be used in ways that enhance the agency's business while maintaining the security of the state's network. These guidelines are intended to help agencies decide whether to use Social Media, and, if the decision is to use this tool, how best to implement the decision.

II. REASONS FOR USING SOCIAL MEDIA

Each agency should take the time to determine how Social Media fits into its communication strategy. When evaluating whether use of Social Media is appropriate, the agency should consider the following:

- How will Social Media enhance outreach and communication with customers, the public, and within the agency?
- How will the agency manage the use of Social Media?
- How will the agency train employees and contractors to use Social Media properly?
- Does the agency have the ability and resources to monitor employees' use of Social Media?
- How will the agency protect confidential information contained in Social Media?
- How will the agency capture and store information generated from Social Media?
- Does the agency have the resources to respond to public records requests arising from use of Social Media?

III. TRAINING

SITSD shall provide agency training on the use of Social Media. Additionally, agencies electing to use Social Media should provide employees training regarding

use of Social Media before the use occurs and continue training as needed. This training should include defining boundaries for using the service and communicating expectations of appropriate use within the workplace. SITSD recommends that agencies document the training and place the documentation in the employee's permanent personnel file.

IV. LAWS AND POLICIES

Agencies and employees using Social Media should comply with applicable Montana and federal laws and State policies. The following laws and policies are examples of those that apply to Social Media use:

- federal and Montana laws prohibiting the disclosure of social security numbers, credit card numbers, certain health care information, and other confidential personally identifiable information;
- federal and Montana laws prohibiting discrimination, harassment, and defamation;
- federal copyright laws and federal and Montana trademark and service mark laws;
- Montana laws and policies addressing the ethical standards of conduct for public employees;
- Montana law regarding access to technology by individuals who are blind or visually impaired (See 18-5-601, MCA, et seq.); and
- State policies regarding the use of email and the internet. These policies include but are not limited to:
 - Statewide Information Systems Policy – User Responsibility
 - Statewide Information Systems Policy – Internet Acceptable Use
 - Statewide Information Systems Policy – SummitNet Acceptable Use.

SITSD recommends that legal counsel and human resources staff be consulted regarding these laws and policies.

V. ACCEPTABLE USE

Work-related communications using Social Media should be professional and consistent with the agency's policies, procedures, and expectations. Inappropriate use of Social Media may be grounds for disciplinary action up to and including termination of employment.

Inappropriate use includes but is not limited to profane language or content; content that promotes or fosters discrimination prohibited under Federal and State law; sexual content or links thereto; and content regarding private business activities or political purposes. Inappropriate use also includes use that is inconsistent with an

agency's mission and its general standards that an employee's work be conducted in a professional and courteous manner.

There is no reasonable expectation of privacy in messages and information transmitted to, received and printed from, or stored on the State's network. An employee should not use the State's network for any matter the employee wants to keep private. (See VII, Public Records, below.)

VI. AGREEMENTS WITH SOCIAL MEDIA PROVIDERS

To the extent consistent with an agency's internal review process, legal counsel should review Social Media service provider agreements before the agency signs the agreement to ensure compliance with Montana law. Some of the common terms and conditions in service provider agreements that bear noting are:

- Indemnification;
- Liability for misuse;
- Dispute resolution;
- Venue for disputes;
- Which state's laws will govern the agreement;
- Ownership of the content located on the Social Media site; and
- Confidentiality provisions

If the agreement with a service provider contradicts Montana law or agency policy, then the service should not be used.

VII. PUBLIC RECORDS

Under Montana law, public records include records in electronic form (§ 2-6-110, MCA). Therefore, communication to or from state personnel through Social Media is likely presumed to be a public record. If a communication is a public record, then the Secretary of State's General Records Retention Schedules provide guidance regarding how long certain types of state government records must be kept. The Secretary of State's website at <http://sos.mt.gov/Records/index.asp> provides information regarding public records and records retention schedules for public records.

A public record is subject to disclosure upon citizen request. See §2-6-102, MCA. Since citizens using state government Social Media sites may be unaware of public record laws, an agency using Social Media should post a statement on the social networking site indicating that communications on the site are presumed to be public records subject to disclosure to third parties.

VIII. SECURITY

Agencies should be aware that the use of Social Media may provide an avenue for anyone with access to the internet to access the Social Media site or the State's network without authorization. The intent of this access may be to damage the State's network or to acquire confidential information about employees or citizens. Given this potential, agencies should educate their employees about the care needed when disclosing information using Social Media and the various attack strategies that hackers use to gain access to systems.

AT A MINIMUM, AGENCIES SHOULD REQUIRE EMPLOYEES USING SOCIAL MEDIA TO ADHERE TO THE FOLLOWING BASIC PRECAUTIONS:

- Read social network services privacy guidelines that are published on their Web sites. Take the time to understand these documents. These documents will include the types of information that the services will reveal or sell to other parties (including spammers). If the terms and conditions of these documents are vague or objectionable, SITSD recommends consultation with legal counsel, human resources staff or SITSD before using the service.
- Create passwords that use both numbers and letters, both upper and lowercase, and special characters for added complexity. Don't share your password with anyone.
- After you type your email address and password into the log-in page, make sure the "Remember me" check box is turned off before you click the log-in button.
- Do not allow your browser to save any passwords.
- Always remember to log-out when finished using the Social Media site.
- Never use personally identifiable or private information on Social Media sites, such as social security numbers, health care information, or information involving individual private personnel matters.
- If a site is hacked, discontinue the site immediately and notify the agency IT department. Indications that the site has been tampered with may include alteration or removal of site graphics or logos, changes to expected functionality, or unapproved content postings.